

How do I login to MIT services that leverage Duo two-factor authentication?

Q: How do I login to MIT services that leverage Duo two-factor authentication?



Touchstone and Duo updates March 22

Touchstone and Duo authentication has been updated with some visual changes and an improved two-factor authentication experience as Information Systems and Technology (IS&T) implemented updates to the Institute's single sign-on web authentication service on Friday, March 22.

- [IS&T News: Touchstone and Duo updates coming March 22](#)
- [Duo Universal Prompt Guide](#)

On this page:

[Authenticating via Touchstone with the Duo authentication requirement enabled](#)

[Duo Push](#)

[Phone Call](#)

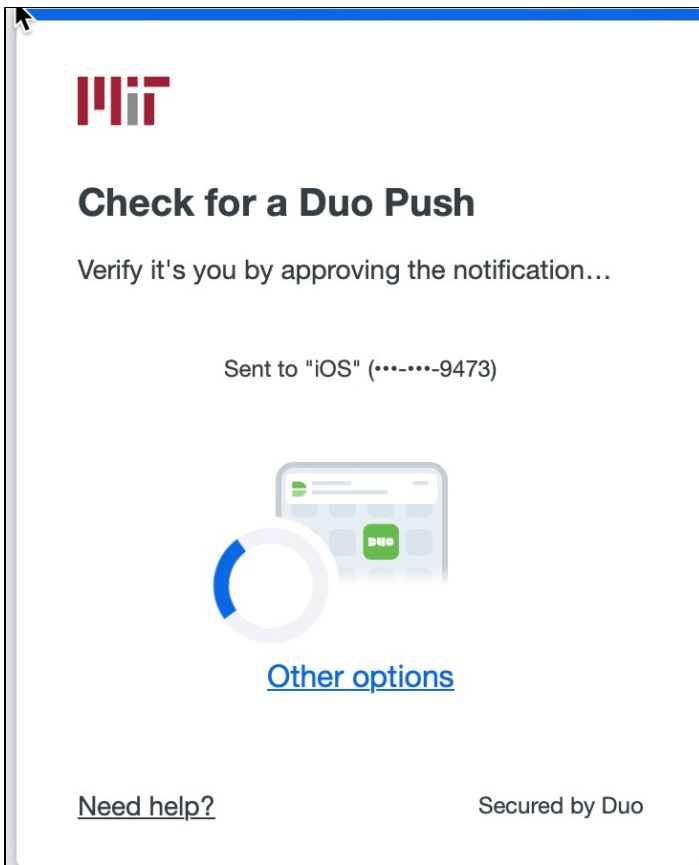
[Passcode](#)

[Connect to a Duo-protected Microsoft Windows machine with Remote Desktop Connection \(RDP\)](#)

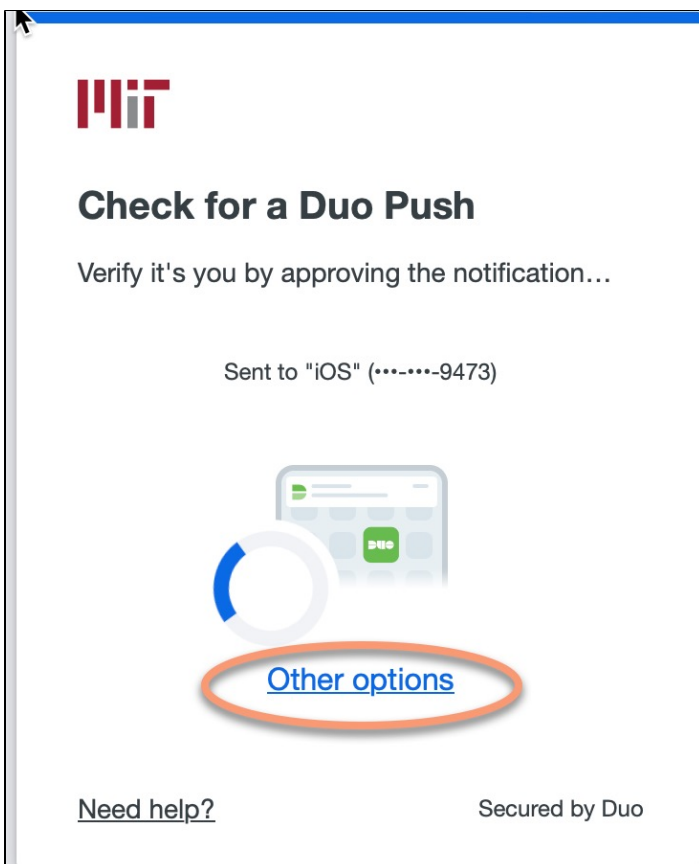
[Acquire Kerberos tickets for a Duo-protected principal using kinit](#)

Authenticating via Touchstone with the Duo authentication requirement enabled

1. Launch a webpage (Chrome, Firefox, Safari and Internet Explorer), that requires Touchstone authentication and begin to authenticate as normal.
2. Once you have completed the Touchstone authentication steps (via Certificates, kerberos tickets or kerberos username and password), the universal Duo prompt will automatically select your preferred authentication method and attempt to authenticate that way. In the case of a Duo Push, it will send one to you without prompting.



-  If you have not selected a preferred authentication method, it will select the one it considers most secure.
3. To choose another authentication method, click the "Other options" link.



Result: A personalized list of other options for authentication will open. Which options appear depend on which authentication methods you set up when you registered for Duo.

[< Back](#)

Other options to log in

Device

All devices ▾



Duo Push
Send to "iOS" (.....9473)

>



Duo Push
Send to ipad (iOS)

>



YubiKey passcode
Enter a code using your YubiKey

>



Hardware token
Enter a code from your hardware token

>



Text message passcode
Send to "iOS" (.....9473)

>



Phone call
Call "iOS" (.....9473)

>



Phone call
Call "Landline" (.....1866)

>



Bypass code
Enter a code from your IT help desk

>



Manage devices
Add a phone, Touch ID, and more.

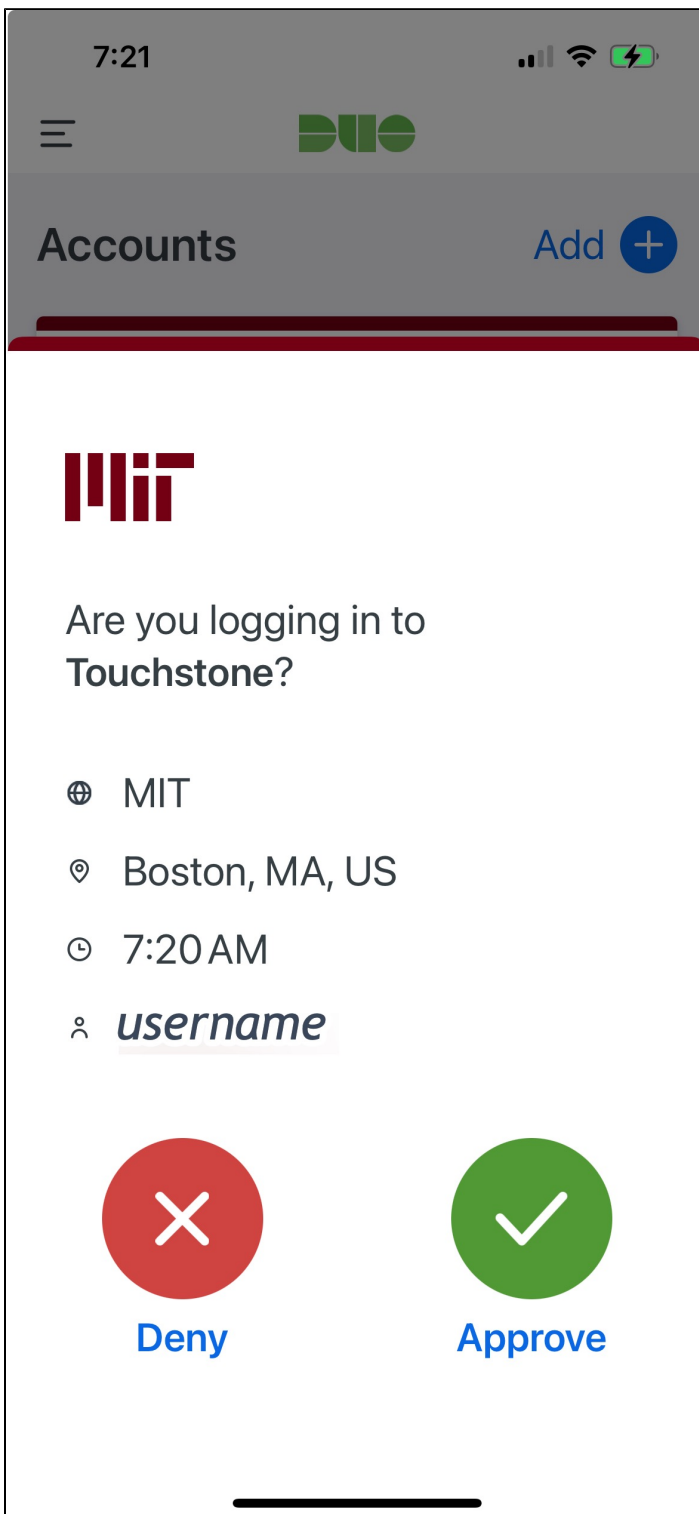
>

 **First you'll verify your identity.**

4. Select the option you want to use to authenticate, and authenticate with that method as usual.

Duo Push

1. If it did not default to this, select "Duo Push" from the options as shown above.
2. A request will be sent to your mobile device via the Duo app
You must have an active mobile (cellular) or wifi connection to receive this request
3. Tap **Approve** on your Mobile Device's Duo app. It should look similar to this:



4. **Result:** Your web browser's Touchstone session should automatically complete authentication



If your mobile phone doesn't automatically show the Duo Push request, you can force a refresh of push requests by tapping and dragging the "MIT" account downwards on your phone.

Phone Call

1. If it did not default to this, select "Phone Call" from the options as shown above.
2. An automated attendant will call your phone
3. Answer and wait for the Duo automated message to begin playing
4. Push any valid dialpad key on your phone (0-9,# or *) and hang-up
5. **Result:** Your web browser's Touchstone session should automatically complete authentication

Passcode



Effective January 23,2024 - Touchstone no longer accepts passcodes from the Duo mobile app as a second authentication factor. Passcodes sent via SMS will be limited to one per message, with a five-minute expiration time.

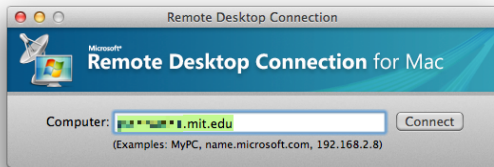
1. If it did not default to this, select "Text message passcode" from the options as shown above.
_Result: The passcode entry screen displays and you will receive a passcode via text message at the number specified.

2. Enter the passcode in the field provided to authenticate. Click **Verify**.

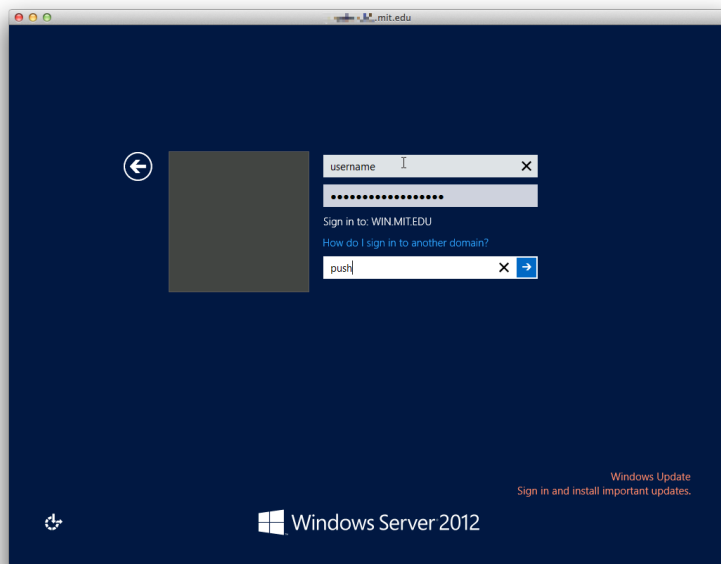
Connect to a Duo-protected Microsoft Windows machine with Remote Desktop

Connection (RDP)

1. Launch Microsoft Remote Desktop and enter the hostname or IP address of the machine you wish to connect to (note: you may have to connect to MIT's VPN service to use RDP).



2. When presented with the Windows login screen, enter your MIT username and password.
3. In the field labeled "Duo Password" you can enter one of the following options:
 - a. **push** - Duo will send a push notification to your registered cell phone with the Duo Security mobile app installed
 - b. **sms** - Duo will send an SMS to your registered cell phone
 - c. **phone** - Duo will call your registered cell phone
 - d. The one time code generated by your hardware token or the Duo Security mobile app (the code changes ever 60 seconds)



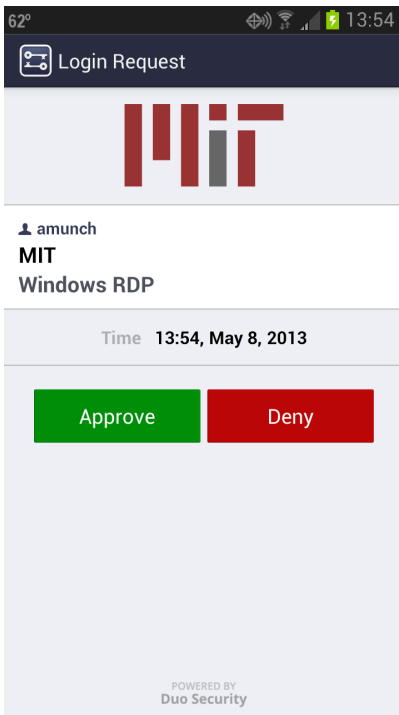
In this example, we've entered "push" in the "Duo Password" field.



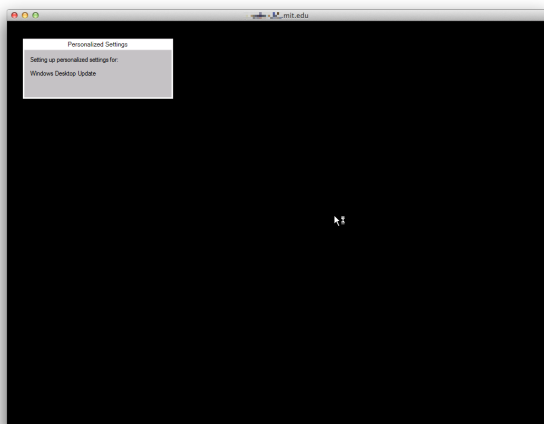
'How to call different devices'

If you have multiple devices that can use the same method, for instance two mobile phones or two phones that can receive phone calls, you can reference them by different numbers. For instance, to call the top device on your managed devices page (<http://duo.mit.edu>), you can use 'phone' (for the default) or 'phone1' to call the second phone, you can use 'phone2'.

4. In this example, you will receive a push notification on your cell phone. Click **Approve**.

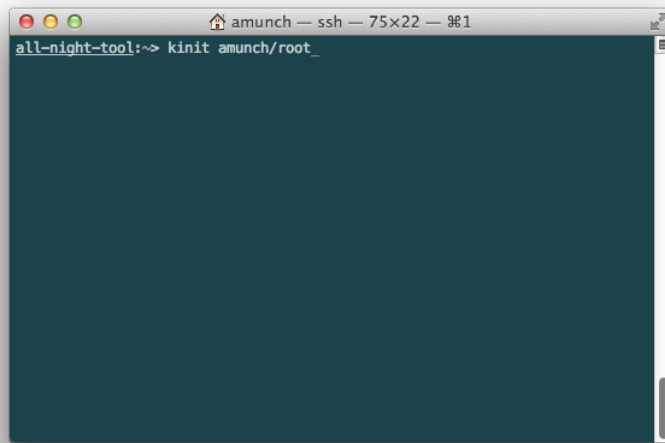


5. The remote Windows system should now complete authentication and the Remote Desktop Connection will complete.



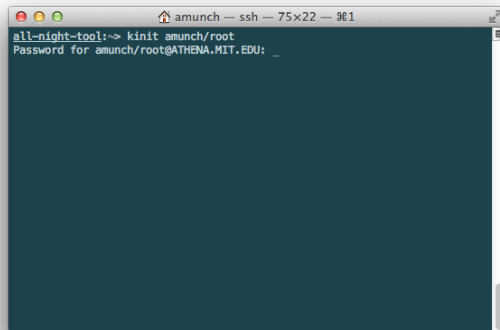
Acquire Kerberos tickets for a Duo-protected principal using kinit

1. Log into an Athena machine (e.g. `ssh athena.dialup.mit.edu`).

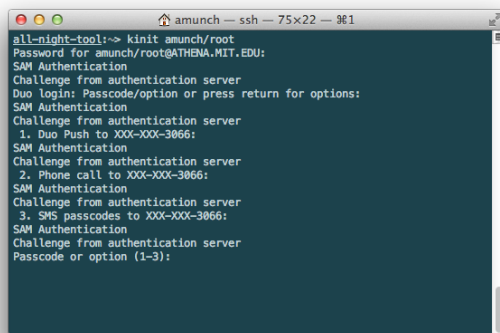


2. Initiate Kerberos ticket acquisition (e.g. `kinit username/root`) and enter the appropriate Kerberos password when prompted.

Note: not all Kerberos accounts will be protected with Duo. Typically, only root accounts or users with escalated privileges (e.g. `username/root` or `username/extra`) will be protected with Duo.



3. The Duo two-factor system will now challenge your login asking for a method to contact you. You can hit the "Enter" key to see all the options available to you. By default, option "1" will send a push notification to the Duo mobile app.



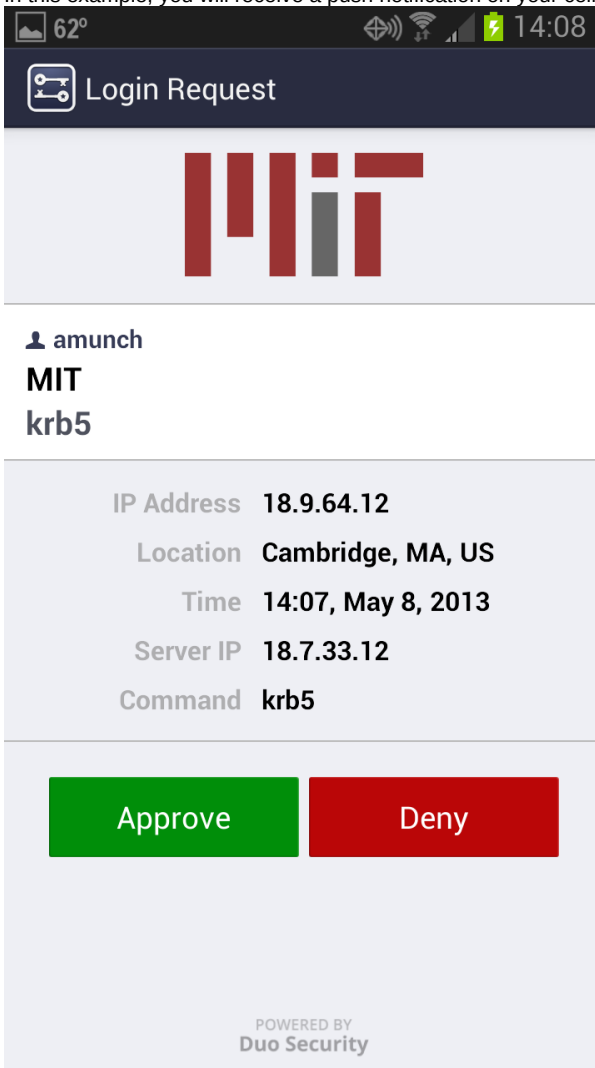
In this example, we've entered "1" as the option.

Note: You will not see any input on the screen as you type.

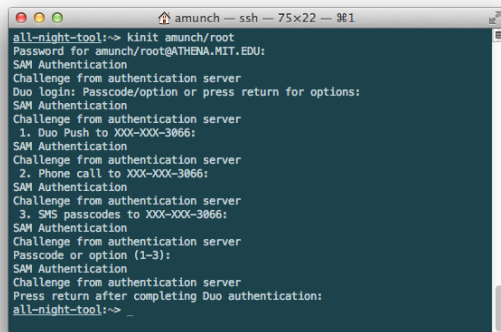
4. Duo will now output, "Press return after completing Duo authentication."

```
amunch — ssh — 75x22 — 981
all-night-tool:~> kinit amunch/root
Password for amunch/root@ATHENA.MIT.EDU:
SAM Authentication
Challenge from authentication server
Duo login: Passcode/option or press return for options:
SAM Authentication
Challenge from authentication server
1. Duo Push to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
2. Phone call to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
3. SMS passcodes to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
Passcode or option (1-3):
SAM Authentication
Challenge from authentication server
Press return after completing Duo authentication: _
```

5. In this example, you will receive a push notification on your cell phone. Click **Approve**.

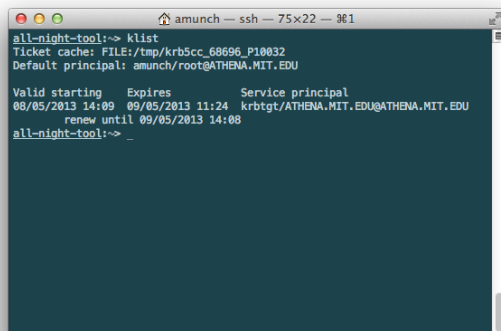


6. Back in your console window, click the **Enter** key.
7. If you have not received any error messages, you should be back at the > prompt and have valid Kerberos tickets.

A terminal window titled 'amunch — ssh — 75x22 — 361' showing the process of logging in as 'amunch/root' on 'ATHENA.MIT.EDU'. The user is prompted for a password and then undergoes Duo authentication. The terminal shows prompts for 'SAM Authentication', 'Challenge from authentication server', and 'Duo login: Passcode/option or press return for options:'. The user selects option 1, 'Duo Push to XXX-XXX-3066', and the process continues with further challenges and a final passcode entry.

```
all-night-tool:~> kinit amunch/root
Password for amunch/root@ATHENA.MIT.EDU:
SAM Authentication
Challenge from authentication server
Duo login: Passcode/option or press return for options:
SAM Authentication
Challenge from authentication server
1. Duo Push to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
2. Phone call to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
3. SMS passcodes to XXX-XXX-3066:
SAM Authentication
Challenge from authentication server
Passcode or option (1-3):
SAM Authentication
Challenge from authentication server
Press return after completing Duo authentication:
all-night-tool:~> _
```

8. You can view your Kerberos tickets by running `klist` from within your console window.

A terminal window titled 'amunch — ssh — 75x22 — 361' showing the output of the 'klist' command. It displays the ticket cache location as 'FILE:/tmp/krb5cc_68696_P10032' and the default principal as 'amunch/root@ATHENA.MIT.EDU'. Below this, it shows a table of valid starting and expiration times for the ticket, along with the service principal 'krbtgt/ATHENA.MIT.EDU@ATHENA.MIT.EDU'.

```
all-night-tool:~> klist
Ticket cache: FILE:/tmp/krb5cc_68696_P10032
Default principal: amunch/root@ATHENA.MIT.EDU

Valid starting    Expires          Service principal
08/05/2013 14:09  09/05/2013 11:24  krbtgt/ATHENA.MIT.EDU@ATHENA.MIT.EDU
                renew until 09/05/2013 14:08
all-night-tool:~> _
```

Also See
[Configuring MacPorts Kerberos for Duo Authentication](#)